UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN RE WASTE MANAGEMENT DATA BREACH LITIGATION	Case No. 1:21-CV-06199-DLC

Plaintiffs' Memorandum of Law in Opposition to Defendant USA Waste Management Resources, LLC's Motion to Dismiss Plaintiffs' Amended Consolidated Class Action Complaint Pursuant to Federal Rule of Civil Procedure 12(B)(6)

TABLE OF CONTENTS

INTRODUCTION 1

STATEMENT OF FACTS 1

LEGAL STANDARD 4

ARGUMENT 4

I. Defendant's efforts to raise conflict of law issues are improper at this stage and Plaintiffs' negligence and breach of confidence claims are properly pled under both New York and Texas law. 4

A. Choice of law questions are not determined at the motion to dismiss stage. 5

B. Should the Court choose to engage in conflict of law analysis, New York law governs plaintiffs' negligence and breach of confidence claims because there is no genuine conflict. 7

II. Plaintiffs Have Properly Alleged Negligence 7

A. Defendant owed Plaintiffs a duty under Texas law. 7

B. The economic loss rule does not apply. 11

III. Plaintiffs have alleged a viable breach of confidence claim 12

IV. Plaintiffs have properly alleged breach of implied contract 13

V. Plaintiffs sufficiently allege a claim for breach of fiduciary duty 15

VI. Plaintiffs sufficiently state a claim for unjust enrichment 17

VII. Plaintiffs have successfully stated a claim under the CCPA 18

A. Plaintiffs properly allege both unauthorized access and exfiltration, theft or disclosure under section 1798.150. 18

B. Plaintiffs satisfied the 30-day notice requirement of the CCPA for alleging damages. 19

C. Plaintiffs sufficiently allege that Defendant failed to cure the CCPA violation. 21

D. Plaintiffs sufficiently allege that Defendant failed to implement reasonable security procedures and practices. 21

VIII. Plaintiffs have successfully stated a UCL claim 23

IX. Plaintiffs have alleged unreasonable delay and incremental damages sufficient to maintain their CCRA claim 24

CONCLUSION 25

TABLE OF AUTHORITIES

Page(s)

Cases

360 Mortg. Grp., LLC v. Homebridge Fin. Servs., Inc.,
No. A-14-CA-00847-SS, 2016 WL 900577 (W.D. Tex. Mar. 2, 2016) 13

Anderson v. Kimpton Hotel & Rest. Grp., LLC,
No. 19-CV-01860-MMC, 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019) 22

Austin v. Kroger Texas, L.P.,
465 S.W.3d 193 (Tex. 2015) 10

Basak v. New York State Dep't of Health,
9 F. Supp. 3d 383 (S.D.N.Y. 2014) 4

Bayerische Landesbank, New York Branch v. Aladdin Cap. Mgmt. LLC,
692 F.3d 42 (2d Cir. 2012) 4

Berly v. D & L Sec. Servs. & Investigations, Inc.,
876 S.W.2d 179 (Tex. App. 1994)..... 8, 9

Blessing v. Sirius XM Radio Inc.,
756 F. Supp. 2d 445 (S.D.N.Y. 2010) 20

Bristol–Myers Squibb Co. v. Matrix Lab'ys Ltd.,
655 F. App'x 9 (2d Cir. 2016) 5, 6

Buchanan v. Rose,
159 S.W.2d 109 (Tex. 1942) 8, 12

Cattie v. Wal-Mart Stores, Inc.,
504 F. Supp. 2d 939 (S.D. Cal. 2007) 20

Cohen v. Ne. Radiology, P.C.,
No. 20 CV 1202 (VB), 2021 WL 293123 (S.D.N.Y. Jan. 28, 2021)..... 14, 15

Cooney v. Chicago Pub. Sch.,
407 Ill. App. 3d 358 (2010).....11

Corsello v. Verizon New York, Inc.,
18 N.Y.3d 777 (2012)..... 18

Cuomo v. Mahopac Nat. Bank,
5 A.D.3d 621 (N.Y. App. Div. 2004) 15

Fero v. Excellus Health Plan, Inc.,
236 F. Supp. 3d 735 (W.D.N.Y. 2017) 17

First Union Nat. Bank v. Paribas,
135 F. Supp. 2d 443 (S.D.N.Y. 2001) 5

Halberstam, Tr. of Zupnick Fam. Tr. 2008 B v. Allianz Life Ins. Co. of N. Am., No.,
16CV6854ARRST, 2017 WL 10187689 (E.D.N.Y. June 9, 2017) 6

Hammond v. The Bank of New York Mellon Corp.,
No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307 (S.D.N.Y. June 25, 2010) 15, 16

Harlow v. Fitzgerald,
457 U.S. 800 (1982) 4

Hyde Corp. v. Huffines,
314 S.W.2d 763 (Tex. 1958) 13

In re Ambry Genetics Data Breach Litig.,
No. SACV2000791CJCKESX, 2021 WL 4891610 (C.D. Cal. Oct. 18, 2021) 15, 16, 24

In re Cap. One Consumer Data Sec. Breach Litig.,
488 F. Supp. 3d 374 (E.D. Va. 2020) 10, 11, 12

In re GE/CBPS Data Breach Litig.,
No. 20 CIV. 2903 (KPF), 2021 WL 3406374 (S.D.N.Y. Aug. 4, 2021) 11, 14

In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., No. CIV.A.,
H-10-171, 2011 WL 1232352 (S.D. Tex. Mar. 31, 2011) 11

Int'l Bus. Machines Corp. v. Liberty Mut. Ins. Co.,
363 F.3d 137 (2d Cir. 2004) 7

Kana Energy Servs., Inc. v. Jiangsu Jinshi Mach. Grp. Co.,
565 S.W.3d 347 (Tex. App. 2018) 13

Kruse v. Wells Fargo Home Mortg., Inc.,
383 F.3d 49 (2d Cir. 2004) 18

Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.,
729 F.3d 421 (5th Cir. 2013) 11

Maag v. U.S. Bank, Nat'l Ass'n,
No. 21-CV-00031-H-LL, 2021 WL 5605278 (S.D. Cal. Apr. 8, 2021) 22

Mayaguez S.A. v. Citigroup, Inc.,
No. 16 CIV. 6788 (PGG), 2018 WL 1587597 (S.D.N.Y. Mar. 28, 2018) 5

MBIA Ins. Corp. v. Countrywide Home Loans, Inc.,
40 Misc. 3d 643 (N.Y. Sup. Ct. 2013)..... 7

McKenzie v. Allconnect, Inc.,
369 F. Supp. 3d 810 (E.D. Ky. 2019).....11

Meadows v. Hartford Life Ins. Co.,
492 F.3d 634 (5th Cir. 2007) 15

Meserole v. Sony Corp. of Am.,
No. 08 CV. 8987 (RPP), 2009 WL 1403933 (S.D.N.Y. May 19, 2009) 5

N. Shore Window & Door, Inc. v. Andersen Corp.,
No. 19CV6194ENVST, 2021 WL 4205196 (E.D.N.Y. Aug. 3, 2021)..... 5, 6

Nelson v. MillerCoors, LLC,
246 F. Supp. 3d 666 (E.D.N.Y. 2017) 18

Odom v. Kroger Texas, L.P.,
No. 3:13-CV-0579-D, 2014 WL 585329 (N.D. Tex. Feb. 14, 2014) 10

Okimoto v. Yougjun Cai,
No. 13 CIV. 4494 RMB, 2015 WL 3404334 (S.D.N.Y. May 21, 2015) 5

Pagayon v. Exxon Mobil Corp.,
536 S.W.3d 499 (Tex. 2017) 10

Rather v. CBS Corp.,
68 A.D.3d 49 (N.Y. App. Div. 2009)..... 15

Razuki v. Caliber Home Loans, Inc.,
No. 17CV1718-LAB (WVG), 2018 WL 6018361 (S.D. Cal. Nov. 15, 2018)..... 22

Rodriguez v. Moerbe,
963 S.W.2d 808 (Tex. App. 1998)..... 8, 9

Sackin v. TransPerfect Glob., Inc.,
278 F. Supp. 3d 739 (S.D.N.Y. 2017) ..... passim

Scheuer v. Rhodes,
416 U.S. 232 (1974) 4

Sonner v. Premier Nutrition Corp.,
971 F.3d 834 (9th Cir. 2020) 23

Speedmark Transp., Inc. v. Mui,
778 F. Supp. 2d 439 (S.D.N.Y. 2011) 5

Thawar v. 7-Eleven, Inc.,
165 F. Supp. 3d 524 (N.D. Tex. 2016) 12

Venetoulias v. O'Brien,
909 S.W.2d 236 (Tex. App. 1995) 8

VL8 Pool, Inc. v. Glencore Ltd.,
No. 20-CV-2053-ALC, 2021 WL 6113981 (S.D.N.Y. Dec. 27, 2021) 4

Wallace v. Health Quest Sys., Inc.,
No. 20 CV 545 (VB), 2021 WL 1109727 (S.D.N.Y. Mar. 23, 2021) 7, 13, 17

Weinberg v. Advanced Data Processing, Inc.,
147 F. Supp. 3d 1359 (S.D. Fla. 2015) 16

Williams v. Albertsons, Inc.,
82 F.3d 415 (5th Cir. 1996) 8

Willingham v. Glob. Payments, Inc.,
No. 1:12-CV-01157-RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013) 11

Statutes

Cal. Bus. & Prof. Code § 17200 23
Cal. Civ. Code § 1798.150(a) 20
Cal. Civ. Code § 1798.150(a)(1) 18
Cal. Civ. Code § 1798.80 24
Cal. Civ. Code § 1798.82(a)(1) 19
Tex. Civ. Prac. & Rem. Code § 134A.002 13

Regulations

2 C.F.R. § 200.79 1

Other Authorities

Restatement (Second) of Torts § 323 (1965) 9

INTRODUCTION

Although Defendant's Motion to Dismiss ("Mot.") offers up myriad reasons why Defendant believes various claims should be dismissed from this case, Defendant's arguments are not persuasive. For example, Defendant argues for the application of Texas law to certain claims even though that argument is clearly premature and unavailing in any event. Defendant also launches attacks on every other claim asserted in the Consolidated Amended Complaint ("CAC")[1], but they are equally futile[2], as explained below. As such, Defendant's motion must be denied.

STATEMENT OF FACTS

USA Waste-Management Resources, LLC ("Defendant" or "Waste Management") allowed cyberthieves to steal sensitive, personally identifiable information ("PII")[3] that its employees, former employees, and their dependents placed in its care. Defendant had (and has) statutory, regulatory, contractual, and common law duties to safeguard that information and to ensure the PII remains protected from unauthorized access. CAC, ECF No. 42, ¶¶ 3, 4, 5, 68, 71, 201. Indeed, the Federal Trade Commission has repeatedly emphasized the need for data security to be factored into all business decision-making. *Id*., ¶ 65. And in a recent Executive Order, President Joe Biden reaffirmed that "the trust we place in our digital infrastructure should be proportional to how trustworthy … that infrastructure is, and to the consequences we will incur if that trust is misplaced." *Id*., ¶ 1. Here, Defendant put that trust in peril by permitting computer

[1] Although the complaint is captioned as a Consolidated Amended Complaint, it is actually the first consolidated complaint filed in this matter.

[2] Plaintiffs, however, are not further pursuing the claim for Breach of Express Contract and do not object to dismissal of that one claim.

[3] Personally identifiable information generally means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79.

hackers to steal the sensitive PII of 268,510 of Defendant's employees, former employees, and their dependents. *Id*., ¶ 2; ECF No. 42-1.

Although Defendant initially detected suspicious activity on its network in January 2021, it was not until months later that Defendant finally determined an unauthorized actor entered Defendant's network environment between January 21 and 23, 2021, and accessed, viewed, and exfiltrated certain data of past and current employees, including full names, Social Security numbers (National IDs), dates of birth, and driver's license numbers (the "Data Breach"). *Id*., ¶¶ 11, 38. Eventually, on May 28, 2021, Defendant began providing notice of the Data Breach to its current and former employees by mailing data breach notice letters (the "Notice Letters") to those individuals whose PII was accessed by unauthorized third parties—a *four-month* delay. *Id*., ¶¶ 12, 39.

Defendant Requires PII as a Condition of Employment. Defendant is a subsidiary of Waste Management, Inc., the largest waste management company in the United States. *Id*., ¶¶ 4, 27. As part of its job application process and as a condition of employment, Defendant requires applicants and employees to provide sensitive PII, including Social Security numbers, driver's license numbers, dates of birth, and addresses. *Id*., ¶¶ 5, 6, 35. Defendant also requires its employees to provide the PII of any dependents. *Id*., ¶ 35.

As a condition of employment, Plaintiffs and Class members entrusted their PII to Defendant and signed the Employee Handbook, which includes the terms and conditions of employment. *Id*., ¶¶ 246, 247. The Handbook includes specific language about employee privacy and the confidentiality of the company's affairs, including the handling and protection of Plaintiffs' and Class members' PII. *Id*., ¶ 248. The Handbook also promises, in part, to safeguard PII as follows: employee PII is treated as "confidential" information; individuals with access to confidential information must protect it from disclosure; confidential information should only be

stored in access–restricted and protected areas; it is only to be shared with authorized people; and unauthorized disclosure is a violation of company policy and may result in legal action against Defendant and/or individuals involved. *Id*., ¶ 248.

Unfortunately, Defendant did not live up to those representations. Rather, Defendant failed to take reasonable and adequate cyber security measures to protect Plaintiffs' and Class members' PII, causing a Data Breach and injuring Plaintiffs and Class members. *Id*., ¶¶ 10, 70, 71, 240, 286, 304, 314, 315.

Defendant's Twelve-Month Credit Monitoring and Identity Protection Services Solution Is Not Adequate Because Risk of Future Harm Persists—Indefinitely. Although Defendant offered twelve months of credit monitoring and identity protection services, credit monitoring is not enough because illicit activity from the Data Breach may occur years after PII exposure, so ramifications are long lasting and severe. *Id*., ¶¶ 51, 197, 207. Because many of the data points stolen are persistent—for example, Social Security number, National ID, name, and date of birth—criminals who purchase the PII belonging to Plaintiffs and the Class members may use the information to commit fraud years later, leaving Plaintiffs and Class members at risk for identity theft indefinitely. *Id*., ¶¶ 51, 204. In fact, in the Notice Letters, Defendant provided "steps you may take to better protect against possible misuse of your personal information," making it reasonable for recipients, including Plaintiffs and Class members, to believe that the risk of future harm (including identity theft) remains substantial. *Id*., ¶ 40.

Plaintiffs and Class Members Have Sustained Injuries. Plaintiffs' action seeks redress for Defendant's negligent handling of PII through its failure to put in place proper safeguards. *Id*., ¶¶ 6, 15. As a result of the Data Breach, Plaintiffs and the Class members have sustained actual, ongoing and imminent injuries that include theft of their PII, ongoing costs associated with the detection and prevention of identity theft, time spent to address and attempt to mitigate

the consequences of the Data Breach, actual fraudulent activity on financial accounts, damages to and diminution in value of their personal data entrusted to Defendant, and the continuing risk of identity theft. *Id*., ¶ 14.

LEGAL STANDARD

In deciding a motion to dismiss, a court must accept all factual allegations in the complaint as true and draw all reasonable inferences in the plaintiff's favor. *See Bayerische Landesbank, New York Branch v. Aladdin Cap. Mgmt. LLC*, 692 F.3d 42, 51 (2d Cir. 2012). "The issue is not whether a plaintiff will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims." *Basak v. New York State Dep't of Health*, 9 F. Supp. 3d 383, 389 (S.D.N.Y. 2014) (quoting *Scheuer v. Rhodes*, 416 U.S. 232, 236 (1974), abrogated on other grounds by *Harlow v. Fitzgerald*, 457 U.S. 800, 102 (1982)). The plaintiffs need only "allege sufficient facts to show 'more than a sheer possibility that a defendant has acted unlawfully[.]' " *VL8 Pool, Inc. v. Glencore Ltd.*, No. 20-CV-2053-ALC, 2021 WL 6113981, at *2 (S.D.N.Y. Dec. 27, 2021).

ARGUMENT

I. Defendant's efforts to raise conflict of law issues are improper at this stage and Plaintiffs' negligence and breach of confidence claims are properly pled under both New York and Texas law.

Rather than argue Plaintiffs cannot state valid negligence and breach of confidence claims under New York law, Defendant concedes those arguments would be unsuccessful, *see* Mot. at 4-5[4], and instead tries to invoke Texas law. But Defendant's argument about choice of law is unquestionably premature and, in any event, wrong. A motion to dismiss is not the place to

[4] Citations to Defendant's motion are to Defendant's internal pagination and not the pagination generated by the ECF filing.

raise fact-intensive choice of law issues. And even if this Court chooses to wade into that question, Defendant has failed to show that the law of the forum should be overridden.

A. Choice of law questions are not determined at the motion to dismiss stage.

Courts in this Circuit are nearly uniform in the holding that a choice of law determination cannot be made at the pleading stage because it is a fact-intensive inquiry. *See Bristol–Myers Squibb Co. v. Matrix Lab'ys Ltd.*, 655 F. App'x 9, 13 (2d Cir. 2016) ("Numerous district courts in this Circuit have concluded that choice-of-law determinations are fact-intensive inquiries that would be premature to resolve at the motion-to-dismiss stage."); *Mayaguez S.A. v. Citigroup, Inc.*, No. 16 CIV. 6788 (PGG), 2018 WL 1587597, at *10 (S.D.N.Y. Mar. 28, 2018) ("[A] choice-of-law determination is premature on this motion to dismiss, since the record lacks facts necessary to conduct the context-specific 'center of gravity' or 'grouping of contacts' analysis required by New York's choice-of-law principles"); *Meserole v. Sony Corp. of Am.*, No. 08 CV. 8987 (RPP), 2009 WL 1403933, at *5 (S.D.N.Y. May 19, 2009) ("[A]t this early stage of the litigation, ... a detailed choice of law analysis would be premature.").[5] As this Court has noted, the choice of law analysis is "'fact intensive and flexible,' and not susceptible to resolution without adequate discovery." *Okimoto v. Yougjun Cai*, No. 13 CIV. 4494 RMB, 2015 WL 3404334, at *4 (S.D.N.Y. May 21, 2015).

[5] *See also N. Shore Window & Door, Inc. v. Andersen Corp.*, No. 19CV6194ENVST, 2021 WL 4205196, at *8 (E.D.N.Y. Aug. 3, 2021) ("Based on the limited record, the Court cannot reasonably determine which jurisdiction's law should apply"); *First Union Nat. Bank v. Paribas*, 135 F. Supp. 2d 443, 453 (S.D.N.Y. 2001) ("[I]t is premature to make a definitive choice of law ruling both because it is not yet clear that there is a conflict between New York and English law and because the litigation is at a preliminary stage"); *Speedmark Transp., Inc. v. Mui*, 778 F. Supp. 2d 439, 444 (S.D.N.Y. 2011) ("[A] choice-of-law determination is premature on [a] motion to dismiss, since the record lacks facts necessary to conduct the context-specific 'center of gravity' or 'grouping of contacts' analysis required by New York's choice-of-law principles.").

Here, there is an insufficient factual record from which the Court can make a choice of law determination for specific claims. And lacking such facts, Defendant's claim that Texas law should apply to certain claims is completely unsupported. Defendant bases its argument entirely on the allegation that its principal place of business is in Texas, while ignoring the allegations that Defendant's state of incorporation is New York, Defendant conducts "substantial business in [New York] through its offices and/or affiliates," and, by inference, New York was the "locus" of Defendant's tort. CAC ¶¶ 27, 32. Defendant also ignores the allegations that Plaintiffs were injured in, and are domiciled in various states, including California, Arizona, Texas, Illinois, Pennsylvania, and Indiana, *id*., ¶¶ 17-26, and that Defendant itself has locations in at least 48 states. *Id*., ¶ 34.

At a minimum, "[b]ased on [this] limited record, the Court cannot reasonably determine which jurisdiction's law should apply." *North Shore Window & Door, Inc.*, 2021 WL 4205196, at *8. And "[w]hen the complaint and its attachments do not contain sufficient allegations to determine which state's law applies, a court must consider whether a [plaintiff] has stated a plausible claim to relief under *any* potentially applicable law." *Halberstam, Tr. of Zupnick Fam. Tr. 2008 B v. Allianz Life Ins. Co. of N. Am.*, No. 16CV6854ARRST, 2017 WL 10187689, at *3 (E.D.N.Y. June 9, 2017) (italics added); *see also Bristol–Myers Squibb Company*, 655 F. App'x at 13 (vacating grant of motion to dismiss "[b]ecause we cannot say that [the plaintiff] has failed to state a claim under at least one of the allegedly applicable laws, nor can we determine at the motion-to-dismiss stage which law indeed governs….")

Here, as noted, Plaintiffs have stated claims under "any applicable law." New York law recognizes an independent duty to protect employees' PII that would "overcome the economic loss rule" in the circumstances alleged in the CAC. Mot. at 4-5 (citing *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 748–49 (S.D.N.Y. 2017)). New York law also allows a breach

of confidence claim when, as here, "a defendant passively fails to protect the data or information at issue." Mot. at 5 (citing *Wallace v. Health Quest Sys., Inc.*, No. 20 CV 545 (VB), 2021 WL 1109727, at *12–13 (S.D.N.Y. Mar. 23, 2021). Since these claims are valid under New York law, a point Defendant itself has conceded, Defendant's request to dismiss Plaintiffs' negligence and breach of confidence claims must be denied.

B. Should the Court choose to engage in conflict of law analysis, New York law governs plaintiffs' negligence and breach of confidence claims because there is no genuine conflict.

Choice of law is irrelevant unless laws of competing jurisdictions are actually in conflict. *Int'l Bus. Machines Corp. v. Liberty Mut. Ins. Co.*, 363 F.3d 137, 143 (2d Cir. 2004). And challengers of the forum's law bear the burden to make this showing. *See MBIA Ins. Corp. v. Countrywide Home Loans, Inc.*, 40 Misc. 3d 643 (N.Y. Sup. Ct. 2013) (placing the burden to assert conflict of law on whichever party challenges the forum's law).

Here, Defendant cannot make that showing. As more fully explained in Sections II and III, *infra*, New York and Texas law do not conflict on the material aspects of negligence and breach of confidence claims. Contrary to Defendant's bald claims, Texas courts have not refused to recognize a duty to protect PII, and likely would recognize that duty, following numerous courts in other jurisdictions and guidance from similar precedent in Texas. *See* Section II, *infra*. Likewise, both Texas and New York have the economic loss rule, but that is not the issue here. In this case, Plaintiffs have not pled solely economic damages and so their claims would not be barred under either state's law. And finally, Defendant attempt does not hold up under scrutiny.

II. Plaintiffs Have Properly Alleged Negligence.

A. Defendant owed Plaintiffs a duty under Texas law.

Defendant argues that "Texas courts have not recognized, and would not recognize, that employers have a duty to protect employee PII from access as a result of a third-party data

breach." Mot. at 14. That is not correct. It has long been the law in Texas "that if a party negligently creates a dangerous situation, it then becomes his duty to do something about it to prevent injury to others if it reasonably appears or should appear to him that others in the exercise of their lawful rights may be injured thereby." *Buchanan v. Rose*, 159 S.W.2d 109, 110 (Tex. 1942); *accord Williams v. Albertsons, Inc.*, 82 F.3d 415 (5th Cir. 1996) ("Texas imposes a duty to act when a party … negligently creates a situation that may injure others."). This duty extends to foreseeable criminal acts of third parties resulting from a defendant's negligence. *See Rodriguez v. Moerbe*, 963 S.W.2d 808, 817 (Tex. App. 1998) (noting there is a duty of care where there is a special relationship between the defendant and the injured party or between the defendant and the third person or when criminal conduct is the foreseeable result of a tortfeasor's negligence); *see also Venetoulias v. O'Brien*, 909 S.W.2d 236, 241 (Tex. App. 1995) ("An actor's negligence is not excused when the criminal conduct is the foreseeable result of the actor's negligence.").

That Texas courts would recognize employers have a duty to protect their employees' PII from third-party data breaches is a logical extension of existing Texas case law. "The common law of torts, including the concept of duty, must evolve in light of the changing conditions and circumstances of society." *Berly v. D & L Sec. Servs. & Investigations, Inc.*, 876 S.W.2d 179, 188 (Tex. App. 1994), *writ denied* (Sept. 29, 1994) (citations omitted). For example, in *Berly*, the trial court granted summary judgment in favor of an employer whose employee was injured by a shoplifter attempting to escape from the custody of another employee. The appellate court reversed, finding that "[i]t is a matter of general and common knowledge that violent crime has become a significant and pervasive social problem. Moreover, the common law recognizes the

duty to take affirmative action to control or avoid increasing the danger from another's conduct that the actor has at least partially created." *Id.* at 188.[6]

The same is true here. It is a matter of general and common knowledge that cybercrime has become a significant and pervasive social problem. *See* CAC, ¶¶ 1, 42, 46, 56, 60-62. Moreover, the PII stored by Defendant—such as Social Security numbers, dates of birth, driver's license numbers, and health information—is particularly valuable and more likely to be targeted by cybercriminals. *See id.*, ¶¶ 41, 47-55. Accordingly, Defendant owed a duty to Plaintiffs because it was reasonably foreseeable that Plaintiffs' PII would be targeted by cybercriminals. *Id.* ¶ 231, 233-34, 236-37.

Moreover, the Texas Supreme Court has adopted Restatement (Second) of Torts § 323 (1965), which provides:

> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if
>
> (a) his failure to exercise such care increases the risk of such harm, or
>
> (b) the harm is suffered because of the other's reliance upon the undertaking.

Colonial Sav. Ass'n v Taylor, 544 S.W.2d116 (Tex. 1976).

While the language of the Restatement references "physical harm," the voluntary duty doctrine and Restatement Section 323 have recently been applied by at least one federal court in

[6] Even Defendant recognizes it has a duty to protect employees from foreseeable criminal conduct. *See* Mot. at 15 ("Employers do not have a duty to … protect employees from third-party misconduct or criminal activity that *is not reasonably foreseeable*.") (emphasis added). Here, Plaintiffs have clearly alleged the criminal conduct at issue was foreseeable. CAC, ¶¶ 1, 42, 46, 56, 60-62, 201, 231, 233. To the extent Defendant disagrees, that is a question for the jury. *See Rodriguez v. Moerbe*, 963 S.W.2d 808, 817 (Tex. App. 1998).

a data breach case. *See In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374 (E.D. Va. 2020) (liability under the voluntary duty doctrine is in lockstep with § 323 of the Restatement (Second) of Torts; allegations that Defendants manifested through its affirmative acts and representations their ability and responsibility to render adequate data protection and failure to do so were adequate to satisfy voluntary undertaking duty doctrine).

Here, Plaintiffs have alleged that "Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and the foreseeable consequences if its data security system were breached." CAC, ¶ 70. This allegation fits squarely within the assumption of duty law where Defendant took possession of the information, knew of the risks of cybercrime, increased the risk of harm by implementing below-standard security measures, and caused Plaintiffs harm.

The cases cited by Defendant do not compel a different result. For example, Defendant cites *Pagayon v. Exxon Mobil Corp.*, 536 S.W.3d 499, 507 (Tex. 2017). But there, the Court found a lack of duty, in part, because "[t]he foreseeability of injury [was] small, and the likelihood of injury [was] remote." *Id.* Defendant also cites *Odom v. Kroger Texas, L.P.*, No. 3:13-CV-0579-D, 2014 WL 585329, at *4 (N.D. Tex. Feb. 14, 2014) for the proposition that employers only "owe employees certain, limited duties related to hiring, supervision, and working conditions." Mot. at 15. But the Texas Supreme Court has been clear that the employment relationship creates additional duties—not fewer. *See Austin v. Kroger Texas, L.P.*, 465 S.W.3d 193, 215 (Tex. 2015) (the employer-employee relationship "may give rise to *additional duties*, such as a duty to provide necessary equipment, training, or supervision.") (emphasis added). Nor does Defendant point to any cases decided under Texas law finding a lack

of duty to safeguard PII.[7] As such, Defendant's argument that Texas would not recognize such a duty is unsupported.

B. The economic loss rule does not apply.

Defendant argues that because Plaintiffs seek recovery for mere economic loss, their negligence claim is barred absent an independent duty (existing outside of contract) to safeguard PII. Mot. at 15-17. This argument is without merit. First, Plaintiffs have clearly alleged more than just economic loss. *See* CAC, ¶ 243(g). Second, as discussed above, Defendant owes an independent duty to Plaintiffs to take reasonable steps to safeguard their PII from the foreseeable criminal acts of third parties.

In support of its argument, Defendant cites two cases in which the plaintiffs chose not to dispute the application of the economic loss rule under Texas law. *See* Mot. at 16-17 (citing *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, No. CIV.A. H-10-171, 2011 WL 1232352, at *21 (S.D. Tex. Mar. 31, 2011) and *Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc.*, 729 F.3d 421, 423 (5th Cir. 2013)). However, Defendant omits any mention of cases finding in an adversarial setting that there *is* an independent duty to safeguard PII under Texas law, and that this independent duty defeats application of the economic loss rule. *See, e.g., In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. at 379.

[7] The only cases cited by Defendant involving a lack of duty to safeguard PII are *Cooney v. Chicago Pub. Sch.*, 407 Ill. App. 3d 358, 361–63 (2010) (no duty under Illinois law) and *Willingham v. Glob. Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *19 (N.D. Ga. Feb. 5, 2013) (no duty under Georgia law). These cases are unpersuasive. The more recent and prevailing position throughout the country is that employers do have an independent duty to safeguard sensitive PII of their employees. *See, e.g., In re GE/CBPS Data Breach Litig.*, No. 20 CIV. 2903 (KPF), 2021 WL 3406374, at *8 (S.D.N.Y. Aug. 4, 2021); *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111-TSH, 2019 WL 7946103, at *11–13 (D. Mass. Dec. 31, 2019); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 818 (E.D. Ky. 2019).

In *Capital One*, the court found the existence of a duty under the Texas Supreme Court's decision in *Buchanan*, stating:

> Here, plaintiffs have essentially alleged that by creating a so-called data lake without adequate safeguards to protect against hacking, Defendants have created a hazardous condition that threatened the Plaintiffs with foreseeable injuries. Based on the principle embraced in *Buchanan*, the Court concludes that if faced with this case, the Texas Supreme Court would recognize a duty separate and apart from the parties' contractual relationship; and for that reason, the Court will not dismiss Plaintiffs' negligence claim under Texas law based on the economic loss rule.

Id. As discussed above, Plaintiffs' allegations are materially similar; because "[D]efendant by [its] own act created the dangerous situation," it had a duty to protect Plaintiffs from reasonably foreseeable harm. *See Buchanan*, 159 S.W.2d at 110.

Finally, Defendant's economic loss argument fails for the basic reason that Defendant disputes the existence of a contractual duty to safeguard PII. *See* Mot. at 18-22. Texas courts are unwilling to apply the economic loss rule at the pleading stage to bar tort claims over the exposure of employee PII where the existence of a contractual duty is in dispute. *See, e.g., Thawar v. 7-Eleven, Inc.*, 165 F. Supp. 3d 524, 532–33 (N.D. Tex. 2016) ("If the policy was part of [the] employment contract, then the economic loss doctrine may well apply to bar her claim. But the Court cannot discern from the Complaint if that is the case and given the Texas Supreme Court's reticence to expand the doctrine beyond the context of products liability and contractual relations, the Court will refrain from dismissing [the] negligence claim at this time.").

III. Plaintiffs have alleged a viable breach of confidence claim.

Defendant argues Texas law treats breach of confidence claims as "synonymous with misappropriation of a trade secret," and requires "affirmative" disclosure to create liability. Mot. at 5. Not so. Texas law does not support Defendant's distinction between "affirmative" and passive disclosure (Tex. Unif. Trade Secrets Act, Tex. Civ. Prac. & Rem. Code § 134A.002.

Subdivision (3)(B)(ii)(b) of § 134A.002 defines the term "misappropriation" as "disclosure [] of a trade secret of another without express or implied consent by a person who: [¶] at the time of disclosure [] knew or had reason to know that the person's knowledge of the trade secret was: [¶] acquired under circumstances giving rise to a duty to maintain the secrecy of or limit the use of the trade secret." *See also Hyde Corp. v. Huffines*, 314 S.W.2d 763, 769 (Tex. 1958).

Although misappropriation in Texas requires "actual use or disclosure" without consent, *see 360 Mortg. Grp., LLC v. Homebridge Fin. Servs., Inc.*, No. A-14-CA-00847-SS, 2016 WL 900577, at *1, *5 (W.D. Tex. Mar. 2, 2016), passive and affirmative disclosures are equally "actual" under Texas law. In *Kana Energy Servs., Inc. v. Jiangsu Jinshi Mach. Grp. Co.*, 565 S.W.3d 347, 353 (Tex. App. 2018), the Texas Court of Appeals defined common-law trade secret claims to include "breach of a 'confidential relationship'" and "disclosure of the trade secret without [victim's] authorization," consistent with section 134A.002. Disclosure can be "affirmative" or otherwise. Accordingly, the disclosure alleged here in the CAC is sufficient to state a claim for breach of confidence under Texas law.

IV. Plaintiffs have properly alleged breach of implied contract.

"Under New York law, a contract implied in fact may result as an inference from the facts and circumstances of the case, though not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct." *Sackin*, 278 F. Supp. 3d at 750. "An implied contract, like an express contract, requires consideration, mutual assent, legal capacity and legal subject matter." *Id.* "The terms of an implied-in-fact contract turn on the conduct of the parties." *Wallace*, 2021 WL 1109727, at *10. Plaintiffs need not plead the precise terms of an implied contract to survive a motion to dismiss. *Id.*

Defendant argues that Plaintiffs' allegations are insufficient to allege the existence of an implied contract because they "allege neither material contract terms nor manifestation of

assent." Mot. at 13. However, in other data breach cases, courts have consistently found factual allegations similar to the ones in this case sufficient to state a claim for breach of implied contract. For example, in *Sackin*, as a condition of employment, the defendant required its employees to submit PII including their names, addresses, dates of birth, Social Security numbers, direct deposit bank account numbers and routing numbers. 278 F. Supp. 3d at 744. After their PII was disclosed in a data breach, a class of employees brought claims for, *inter alia*, breach of implied contract. The court denied the employer's motion to dismiss, noting that the employer "required and obtained the PII as part of the employment relationship, evincing an implicit promise by [the employer] to act reasonably to keep its employees' PII safe." *Id.* at 750. The court further explained, "[w]hile [Defendant] may not have explicitly promised to protect PII from hackers in Plaintiffs' employment contracts, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently." *Id.* at 751 (internal quotations omitted).

Other courts have reached the same result. *See, e.g.*, *In re GE/CBPS Data Breach Litigation*, 2021 WL 3406374, at *12 (plaintiff properly alleged breach of implied contract claim by asserting that he and the proposed class members provided Canon with their PII as a condition of their employment, and that Canon failed to safeguard and protect their PII or provide timely and accurate notice that their PII was compromised in a data breach); *Cohen v. Ne. Radiology, P.C.*, No. 20 CV 1202 (VB), 2021 WL 293123, at *9 (S.D.N.Y. Jan. 28, 2021) (denying defendants' motion to dismiss breach of implied contract claim where plaintiff alleged that defendants obtained, created, and maintained personal health information as part of providing radiological services to their patients, evincing an implicit promise by defendants to protect their patients' data from unauthorized users).

Contrary to Defendant's argument, Plaintiffs have alleged the material terms of the implied contract and mutual assent. A breach of implied contract claim is not dependent on the express words of the parties. Rather, "[u]nder New York law, a contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct." *Cohen*, 2021 WL 293123, at *8. Defendant required and obtained the PII as part of the employment relationship, evincing its implicit promise to act reasonably to safeguard and protect its employees' PII. It cannot credibly be argued that when employees provide their PII to their employer there is not an expectation by both parties that the employer will protect that PII from unauthorized disclosure, as recognized by the court in *Sackin*.

V. Plaintiffs sufficiently allege a claim for breach of fiduciary duty

Defendant contends that employers do not "generally" owe fiduciary duties to their employees under New York and Texas law. However, none of the cases cited by Defendant addresses the situation where employees have entrusted their highly sensitive PII to their employer as a condition of their employment and the employer subsequently failed to take reasonable measures to protect that information from unauthorized disclosure[8]. Defendant argues that "the fact that Plaintiffs provided WM with their PII in connection with their employment does not create such a duty." Mot. at 16. Notably, however, the cases Defendant cites in support

[8] *See Rather v. CBS Corp.*, 68 A.D.3d 49, 55 (N.Y. App. Div. 2009) (involving action by employee against employer related to employment contract termination); *Meadows v. Hartford Life Ins. Co.*, 492 F.3d 634, 640 (5th Cir. 2007) (finding no fiduciary relationship where former employee brought action against employer with respect to claims the employer had purchased life insurance policies for said employee for its own benefit); *Cuomo v. Mahopac Nat. Bank*, 5 A.D.3d 621 (N.Y. App. Div. 2004) (evaluating whether fiduciary relationship existed between loan borrowers and defendant bank); *Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *10 (S.D.N.Y. June 25, 2010) (action brought by consumers against the Bank of New York Mellon Corporation relating to data breach); *In re Ambry Genetics Data Breach Litig.*, No. SACV2000791CJCKESX, 2021 WL 4891610, at *7 (C.D. Cal. Oct. 18, 2021) (action by customers against companies that provided genetic testing services arising from data breach).

of that statement are data breach actions brought by *consumers*, and thus, do not address the employee-employer relationship. *See Hammond*, 2010 WL 2643307, at *10; *In re Ambry Genetics Data Breach Litigation*, 2021 WL 4891610, at *7; *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1367 (S.D. Fla. 2015) (action by ambulance patients against medical billing company).

While the employer-employee relationship may not automatically give rise to a fiduciary duty, it can result in the imposition of fiduciary duties depending on the facts of the case. Here, Plaintiffs have sufficiently alleged a fiduciary relationship between Defendant and its employees with respect to the protection of their highly sensitive PII, which was stolen by hackers as a result of Defendant's failure to implement reasonable measures to ensure the protection of Plaintiffs' PII. CAC, ¶¶ 7, 66, 203, 233, 243, 277-83. *See also Sackin*, 278 F. Supp. 3d at 747–48 (recognizing a common law duty under New York law on the part of an employer to safeguard its employees' PII and stating "employers have a duty to take reasonable precautions to protect the PII that they require from employees" because employees "ordinarily have no means to protect that information in the hands of the employer, nor is withholding their PII a realistic option").

Secondly, Defendant argues that Plaintiffs' fiduciary duty claim is subject to dismissal because it is "entirely duplicative of their implied contract claim." Mot. at 16. However, the allegations in support of Plaintiffs' fiduciary duty claim are not expressly raised in Plaintiffs' breach of contract claim. Plaintiffs' fiduciary duty claim is based on Defendant assuming a fiduciary duty by undertaking to guard its employees' PII and to act primarily for the benefit of those employees. This assumed fiduciary duty included the obligation to safeguard the PII and to timely detect and notify them in the event of a data breach. These standards are separate from the breach of contract claim.

VI. Plaintiffs sufficiently state a claim for unjust enrichment

"In order to adequately plead such a claim, the plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." *Sackin*, 278 F. Supp. 3d at 751. The Complaint adequately alleges all three elements—first, that Waste Management received the benefits of Plaintiffs' labor; second, that Waste Management was enriched at Plaintiffs' expense when it failed to implement security measures to protect Plaintiffs' PII which Defendant required and obtained in the course of Plaintiffs' employment; and third, that it would be inequitable and unconscionable to allow Waste Management to retain the money it saved by maintaining inadequate data-security, while leaving Plaintiffs to suffer the consequences. *Id.*

Contrary to Defendant's argument, the unjust enrichment claim is not precluded by Plaintiffs' breach of contract claims. "[W]here a bona fide dispute exists as to the existence of the contract, the plaintiff may proceed on both breach of contract and quasi-contract theories." *Id.* As stated by the Court in *Sackin*, "although the Complaint adequately pleads an implied-in-fact contract, Defendant's opposition suggests that it will dispute that Defendant agreed to be bound in an implied contract with Plaintiffs." *Id.* at 751–52; *see also Wallace*, 2021 WL 1109727, at *11 ("[B]ecause defendant disputes whether a contract exists, plaintiffs may proceed with their claims for both breach of implied contract and unjust enrichment."); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 770 (W.D.N.Y. 2017) (declining to dismiss unjust enrichment claim where "the parties dispute whether the parties have an enforceable contract with definite and material terms regarding the provision of data security").

Defendant also claims that Plaintiffs' unjust enrichment claim is barred as duplicative of Plaintiffs' other tort and statutory claims. This is both unavailing and not ripe for decision at this

stage in the litigation. New York courts have been hesitant to dismiss claims that may seek duplicative relief at the motion to dismiss stage.[9]

While courts have held that claims for unjust enrichment "will not survive a motion to dismiss where plaintiffs fail to explain how their unjust enrichment claim is not merely duplicative of their other causes of action," *Nelson v. MillerCoors, LLC*, 246 F. Supp. 3d 666, 679 (E.D.N.Y. 2017), such is not the case in the CAC here. Even if Plaintiffs' other causes of action were for some reason unsuccessful, Plaintiffs could still prove their unjust enrichment claim if it is determined that Defendant "received a benefit ... that ought to in 'equity and good conscience' be turned over to [Plaintiffs]." *Nuss v. Sabad*, No. 10-cv-0279, 2016 WL 4098606, at *11 (N.D.N.Y. July 28, 2016) (quoting *Corsello v. Verizon New York, Inc.*, 18 N.Y.3d 777, 790 (2012)).

VII. Plaintiffs have successfully stated a claim under the CCPA

A. Plaintiffs properly allege both unauthorized access and exfiltration, theft, or disclosure under section 1798.150.

Plaintiffs have shown that their information was accessed by an unauthorized individual carrying out the Data Breach and that the individual took Plaintiffs' PII. Defendant wrongly claims that Plaintiffs have not shown that Plaintiffs' personal information was subject to both unauthorized access **and** "exfiltration, theft, or disclosure." Cal. Civ. Code § 1798.150(a)(1). Throughout their CAC, Plaintiffs allege both of these elements of this section of the CCPA. For example, "the actual and imminent injuries suffered by Plaintiffs and the proposed Class as a

[9] *See, e.g.*, *Membler.com LLC v. Barber*, No. 12-CV-4941 JS GR, 2013 WL 5348546, at *14 (E.D.N.Y. Sept. 23, 2013) ("At the pleading stage, Plaintiff is not required to guess whether it will be successful on its contract, tort, or quasi-contract claims…. While Plaintiff's unjust enrichment and conversion claims may ultimately seek duplicative relief, at [the motion to dismiss] stage the Court will not dismiss the unjust enrichment claim."). The Federal Rules permit pleading in the alternative. *See Kruse v. Wells Fargo Home Mortg., Inc.*, 383 F.3d 49, 55 n.3 (2d Cir. 2004) (noting that the Federal Rules "permit[ ] pleading inconsistent theories in the alternative").

direct result of the [D]ata [B]reach include . . . theft of their personal data." CAC, ¶ 14. Contrary to Defendant's claims, Plaintiffs do not just make conclusory statements; instead, Plaintiffs make specific allegations of unauthorized access: "As reported by Defendant, between January 21 and January 23, 2021, an unauthorized actor entered [Defendant's] environment and accessed and took a number of files . . . . On May 4, 2021, and during the weeks following, Defendant determined that the Data Breach included files containing sensitive PII, including data of employees and former employees (and their dependents), such as names, Social Security numbers (or National IDs), dates of birth, and driver's license numbers." *Id.*, ¶ 11 (emphasis added). This information was reported through a letter that Defendant sent to States' Attorneys General and Plaintiffs. *Id.*, ¶¶ 2, 39, 40, 73, 85, 97, 110, 122, 136, 148, 161, 172, 186. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on or about May 28, 2021, evidencing that the exposed data was unencrypted and exposed to theft, exfiltration, or disclosure. CAC, ¶ 7. As such, Plaintiffs have shown that Defendant's Data Breach is within the scope of the CCPA.

B. Plaintiffs satisfied the 30-day notice requirement of the CCPA for alleging damages.

Defendant claims that Plaintiffs did not provide it with the required statutory notice, Mot. at 20 and n.7, but Plaintiffs did. First, under the plain language of the CCPA, it is not necessary to send the 30-day notice before filing a complaint as Defendant claims; the 30-day notice is only necessary before seeking statutory damages: "Prior to initiating any action against a business **for statutory damages** on an individual or class-wide basis, a consumer shall provide a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have

been or are being violated." Cal. Civ. Code § 1798.150(a) (emphasis added.) Here, the CCPA claims in the original complaints did not seek damages but only injunctive or other equitable relief. *See Fierro v. USA Waste-Management Resources, LLC*, *et al*., No. 1:21-cv-06147 (S.D.N.Y. filed July 19, 2021), ECF No. 1, ¶ 150; ECF No. 1 (*Marcaurel* Complaint), ¶ 173.

Second, the operative complaint here is the CAC, filed nearly five months later on August 2, 2021, well beyond the required 30-day notice period. In the CAC, Plaintiffs did allege statutory damages, but only after Plaintiffs sent written 30-day notices to cure to Defendant on June 21, 2021 and July 19, 2021. CAC, ¶ 307.

Courts addressing a similar pre-suit notice requirement in the California Consumers Legal Remedies Act ("CLRA") have held that a complaint alleging only injunctive relief that is filed before or simultaneously with the sending to defendant of a notice to cure is not subject to dismissal for failure to satisfy the pre-suit notice requirement. For example, in *Blessing v. Sirius XM Radio Inc.*, 756 F. Supp. 2d 445 (S.D.N.Y. 2010), the plaintiffs amended their complaint to add a CLRA cause of action and sent the required 30-day notice to defendant to cure the CLRA violations. *Id.* at 457–58. Later, the plaintiffs amended again to allege damages under the CLRA *after* the violation was not cured. *Id*. The court found that the underlying purpose of the notice requirement was satisfied because defendant received adequate notice, through the letter and the complaint, even though the notice came after the complaint was filed. *Id.*[10]

Here, the CCPA has a similar requirement that is designed to give defendants an opportunity to cure before plaintiffs can seek statutory damages. In this case, Plaintiffs satisfied

[10] *Cattie v. Wal-Mart Stores, Inc.*, 504 F. Supp. 2d 939, 949–50 (S.D. Cal. 2007) is distinguishable. The plaintiff in that case sought statutory damages *before* sending a 30-day notice and the court found that the CLRA 30-day notice requirement was therefore not satisfied. However, the court in *Cattie* acknowledged that a consumer alleging CLRA violations could bring an action for injunctive relief without giving notice and then later amend to request damages once thirty days had passed from sending the letter. *Id.* at 949–50. That is exactly what Plaintiffs did here.

the pre-suit notice requirement by alleging only injunctive or other equitable relief in their original complaints, sending Defendant notice to cure letters, and waiting at least 30 days to amend and allege damages. *See*, *e.g.,* ECF No. 1, ¶¶ 151, 174; CAC, ¶ 307. The CCPA clam is therefore not subject to dismissal.

C. Plaintiffs sufficiently allege that Defendant failed to cure the CCPA violation.

Defendant wrongly blames Plaintiffs for its failure to cure the CCPA violations. Defendant claims that Plaintiffs "plead no facts contradicting the assertions in WM's responses to their CCPA notice letters that it has cured the noticed violations and that no further violations shall occur." Mot. at 28. However, none of the measures mentioned in Defendant's CCPA response letter is a cure that will protect Plaintiffs' PII that has already been released. CAC, ¶¶ 44-45. Plaintiffs allege substantive facts of what should have happened before the breach. Plaintiffs allege that Defendant could have, but failed to, implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and Class members' PII. *Id.*, ¶¶ 37-40, 63-71, 201-03. Defendant did not include in its response any recognition of these security measures. Notably, Defendant also did not include in its response a reason why Plaintiffs' PII was unencrypted, as Plaintiffs allege, nor did Defendant claim to have subsequently encrypted Plaintiffs' or Class members' PII. Mot. Ex. B. As such, Plaintiffs' claim for statutory damages under the CCPA must stand because Plaintiffs adequately alleged that Defendant did not cure its violation of the CCPA when it failed to implement reasonable security measures, such as encryption, to protect Plaintiffs' personal information.

D. Plaintiffs sufficiently allege that Defendant failed to implement reasonable security procedures and practices.

Plaintiffs allege that Defendant should have implemented several reasonable security procedures, including following guidance from the FTC that recommends that businesses should

delete personal information that is no longer needed and encrypt information stored on computer networks. CAC, ¶ 66. These are the most basic and reasonable security procedures and practices that an organization can take, yet Defendant has not disputed Plaintiffs' claims regarding its lack of these security procedures. Instead, Defendant points to several cases where the Plaintiff did not allege any lack of reasonable security protocols. *See Maag v. U.S. Bank, Nat'l Ass'n*, No. 21-CV-00031-H-LL, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021) (holding that plaintiff failed to allege any facts to support the notion that Defendant's security was deficient where Plaintiff ***only*** alleged that Defendant did not "implement and maintain reasonable security procedures and practices" and "failed to effectively monitor its systems for security vulnerabilities"); *Anderson v. Kimpton Hotel & Rest. Grp., LLC*, No. 19-CV-01860-MMC, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019) (dismissing plaintiffs' CLRA claim because plaintiffs "fail[ed] to allege ***any*** facts in support of their conclusory allegation that" defendant did not implement reasonable security protocols) (emphasis added); *Razuki v. Caliber Home Loans, Inc.*, No. 17CV1718-LAB (WVG), 2018 WL 6018361, at *2 (S.D. Cal. Nov. 15, 2018) (dismissing plaintiff's CCRA claim because plaintiff's allegations "recited a few buzz words," rather than factual allegations showing how defendant's procedures were noncompliant).

Here, in contrast to the cases Defendant cited, Plaintiffs allege facts showing that Defendant failed to implement some of the most basic security measures, such as encryption and deleting PII it no longer needed. Plaintiffs allege that Defendant was required to notify Plaintiffs of a data breach if their information was unencrypted, and Defendant did, evidencing that Plaintiffs' information was unencrypted. CAC, ¶ 7, n.5. Plaintiffs also allege facts demonstrating that Defendant failed to delete PII that was no longer needed, *i.e.*, Plaintiff Marcaurel was employed with Defendant over 20 years ago and received a notice that her PII was compromised in Defendant's Data Breach. *Id.*, ¶¶ 72-73. As such, Plaintiffs went beyond "mere buzz words"

and alleged enough facts to show that Defendant did not implement reasonable security measures.

VIII. Plaintiffs have successfully stated a UCL claim

Plaintiffs have also properly stated a claim for Defendant's violation of Cal. Bus. & Prof. Code § 17200, *et seq.* (the "UCL") seeking injunctive relief. Defendant claims that the UCL claim should be dismissed because Plaintiffs did not allege that they lack an adequate remedy at law, citing *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). However, as a court recently held following *Sonner*, "[p]laintiffs are not barred from seeking equitable relief in the form of an injunction under the UCL." *Brooks v. Thomson Reuters Corp.*, 2021 U.S. Dist. LEXIS 154093, at *33 (N.D. Cal. Aug. 16, 2021).[11] As Judge Chen recognized, "courts have declined to apply *Sonner* to bar UCL claims for injunctive relief, recognizing that the prospect of paying damages is sometimes insufficient to deter a defendant from engaging in an alleged unlawful, unfair, or fraudulent business practice." *Brooks*, 2021 U.S. Dist. LEXIS 154093, at *34-35 (collecting cases and noting that damages for past conduct does not necessarily dissuade future behavior). In fact, the Ninth Circuit expressly observed that "[i]njunctive relief [was] not at issue" in *Sonner* because the defendant only moved to dismiss the plaintiff's restitution claims. *Id.*, 971 F.3d at 842. Here, Plaintiffs seek Defendant's implementation of 20 different types of security measures as a form of injunctive relief. CAC, ¶¶ 76-78. For example, Plaintiffs ask the court to "[require] Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiffs' and Class members'

[11] *Sonner* is also factually distinguishable since there, on the eve of trial, plaintiff sought to secure a bench trial under the UCL by forgoing CLRA damages claims despite the court's direct warning, and later sought to add those same damages claims. *See Rothman v. Equinox Holdings, Inc.*, 2021 U.S. Dist. LEXIS 80683, at *34 (C.D. Cal. Apr. 27, 2021) (noting that, "unlike *Sonner*, this matter is not currently on the eve of trial and . . . there is, at present, no pending motion for injunctive relief that would require the Court to determine the adequacy of plaintiff's legal remedies.").

PII" and "[require] Defendant to engage independent third-party security auditors/penetration testers" to conduct security checks. *Id.*, ¶¶ 76-78. These measures will prevent future harm by strengthening Defendant's security to protect the PII belonging to Plaintiffs, Class members, and future employees or individuals who provide such information to Defendant. Plaintiffs have properly pled their UCL claim.[12]

IX. Plaintiffs have alleged unreasonable delay and incremental damages sufficient to maintain their CCRA claim

Plaintiffs allege that Defendant violated the California Consumer Records Act ("CCRA"), Cal. Civ. Code § 1798.80, because it unreasonably delayed (not less than 65 days) informing California Plaintiffs and California Class members about the Data Breach affecting their PII after Defendant knew the Data Breach had occurred. CAC, ¶ 328. Indeed, Plaintiffs allege that Defendant first detected the Data Breach on or about January 21, 2021, yet failed to notify California Plaintiffs and California Class members until May 28, 2021—four months and one week later. *Id.*, ¶¶ 37, 39. Plaintiffs allege very clearly that Defendant knew about the breach as of January 21, 2021, when Defendant detected suspicious activity, an allegation Defendant does not dispute. *Id*. Defendant's argument, that Plaintiffs failed to allege an unreasonable delay in Defendant's notice to Plaintiffs and California Class members, must therefore fail as Plaintiffs allege a delay of over four months, not the three weeks Defendant attempts to claim by parsing the difference between detecting the breach and determining the exact details of that breach. *See Id*.

Defendant also argues that Plaintiffs lack statutory standing to assert a claim under the CCRA due to not alleging harm traceable to Defendant's unreasonable delay in notifying them about the Data Breach because Plaintiffs did not specifically allege that their harms increased

[12] *In re Ambry Genetics Data Breach Litigation*, 2021 WL 4891610, at *8, is distinguishable because in that case the plaintiffs' UCL claim sought only to remedy past harm and not future harm.

incrementally as a result of the Data Breach. However, such argument ignores both Plaintiffs' allegations and the law. Plaintiffs allege that as a result of Defendant's unreasonable delay in notifying them about the Data Breach they were "deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze." CAC, ¶ 332. Plaintiffs also allege that "California Plaintiffs and California Class members [experienced] incrementally increased damages separate and distinct from those simply caused by the Data Breach itself." *Id*., ¶ 333.

CONCLUSION

With the exception of the breach of express contract claim, Defendant's motion to dismiss should be denied. Defendant has not shown any entitlement to the dismissal of the remaining claims.

DATED: January 28, 2022

CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP

/s/ Gayle M. Blatt

Gayle M. Blatt (*pro hac vice*)
Michael Benke
110 Laurel Street
San Diego, CA 92101-1486
Tel: (619) 238-1811
Fax: (619) 544-9232
gmb@cglaw.com

Lead Plaintiffs' Counsel